Section:	06	Title:	Information Security
Sub Section:	03	Title:	Information Security
Document:	04	Title:	Virus Protection

1. STANDARD

To insure data integrity and uninterrupted service, virus-checking programs approved by the ISD Security will be continuously enabled on all networked servers and networked personal computers.

1.1. Summary of Standard Changes

1.2. Purpose

The intention of this standard is to keep all software used on ISD systems free from viruses, worms, Trojan horses, and other unauthorized programs, and thereby assuring continued uninterrupted service.

1.3. Scope

Applies to all software used in ISD and the systems upon which it runs.

1.4. Responsibilities

1.5. Definitions and Abbreviations

1.6. Description of Standard

Virus protection software will be found and installed, running in continuous mode on all applicable systems. The software will be upgraded or replaced as needed. Detection of problems will be immediately reported to ISD Security with no penalty. No virus type software will be produced at ISD.

1.7. Implications

ISD Security, in conjunction with the Local Area Network Group, will find the best virus checking programs available for ISD use and will ensure that the software is upgraded and/or replaced by more effective software as it becomes available. ISD will virus check all software or other necessary communication entities placed on ISD systems.

1.8. References

1.9. Attachments

2. VIRUS, WORM, AND TROJAN HORSE PROTECTION PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. ISD Security, in conjunction with the Local Area Network Group, will identify standard virus protection software packages which meet ISD needs. The emphasis will be on networked and small systems.

2.2.2. Protection software will provide continuous checking on network software, and will be 'continuously enabled' on individual workstations.

2.2.3. When an employee detects a virus, worm, or trojan horse, they will immediately report it to ISD Security. Upon notice, even if their negligence was a contributing factor, no disciplinary action will be taken.

2.2.4. Employees who do not report virus, or like infections will be subject to disciplinary action.

2.2.5. No employee with intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.

2.2.6. All software and files down-loaded from non-ISD sources via the Internet (or any other public or private source) will be screened with virus detection software. This screening will take place prior to being run or examined via another program such as a word processing package.

2.2.7. Software to be installed on ISD systems will be screened. A secure copy of the software will be kept on disk, or other format outside and exclusive from ISD systems

2.3. References

2.4. Attachments